NORTEL

NSNA
Software Release 2.1.1.1

1. Release Summary

Release Date: July 2009
Purpose: Software maintenance release to address customer software issues.

2. Important Notes before Upgrading to This Release

NSNAS Software Upgrade Requirements:

NSNAS should have installed with version 1.6 or later before upgrade.

Saved Configuration file compatibility

In order to maximize configuration compatibility during upgrade, Nortel do not recommend upgrading from very old manufacturing releases like 1.0 or 1.5 to 2.1.X based release. Please do interim upgrade to 2.0.X based release before upgrading to 2.1.1.1.

3. Platforms Supported

4050, 4070

4. Notes for Upgrade

File Names for This Release

File Name	Module or File Type	File Size (bytes) & MD5
NSNAS-2.1.1.1-upgrade_complete.pkg	Upgrade image	49,561,701 (bytes) 94c70cff579b039725a69b06667a6c27
NSNAS-2.1.1.1-cdimage.iso.gz	Compressed ISO image	51, 867,406 (bytes) 27c4f56ef9382330785bce56f64874f2
NSNAS_MIBs_2.1.1.1.zip	NSNAS SNMP MIBs	163,177 (bytes) e259af81db441efe430980735a34edf4
NSNAS_TPS-2.1.1.1.tgz	NSNAS TPS Module	7,612 (bytes) fd9ddb39a92c79af57a3ed9ce4b6931f
NSNAS-2.1.1.1-boot.img	NSNAS Network Boot image	49,533,900 (bytes) 9b597f3ca3304116bf9b0de79b07b810

5. Version of Previous Release

Software Version 2.1.1.0

6. Compatibility

7. Changes in This Release

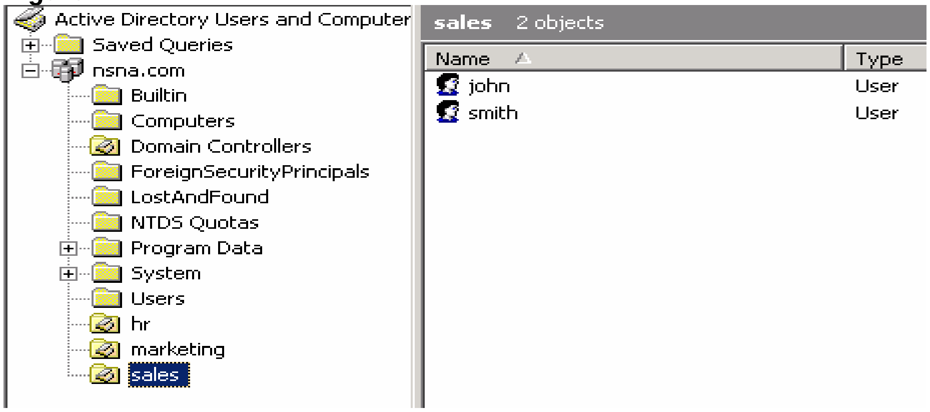
Enhancements in This Release

Support for LDAP "Organization Unit" as user group (Q02045129)

This enhancement enables Nortel SNAS to extract any part of a Distinguished Name (DN) as the user group name. Prior to this release always the initial part of DN is extracted as user group name if Short Group Format is enabled. This enhancement introduces a new LDAP authentication server configuration item Short Group Attribute with which administrator can specify any part of DN to be extracted as group name. Short Group Attribute setting will be effective only when Short Group Format is enabled. If Short Group Attribute is not configured (is empty string) group name extraction will be performed as same as in the releases prior to NSNAS 2.1.1.1. A sample scenario where this enhancement is applicable is described below

Consider LDAP directory structure as shown in below picture in which users are added into their respective organization unit hr, marketing and sales.

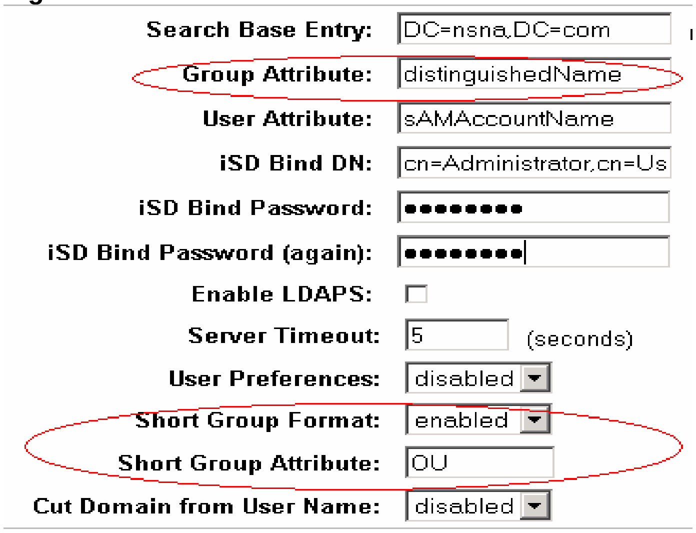
Figure 1



Name	Type
john	User
smith	User

If administrator wants to use the Organization Unit name as group name without explicitly adding users to a Group object (or without adding memberOf attribute of User object), the new LDAP Authentication Server configuration will help administrator to achieve that. Below figure shows a sample configuration

Figure 2



Search Base Entry:	DC=nsna,DC=com
Group Attribute:	distinguishedName
User Attribute:	sAMAccountName
iSD Bind DN:	cn=Administrator,cn=Us
iSD Bind Password:	●●●●●●●●●
iSD Bind Password (again):	●●●●●●●●●
Enable LDAPS:	□
Server Timeout:	5 (seconds)
User Preferences:	disabled
Short Group Format:	enabled
Short Group Attribute:	OU
Cut Domain from User Name:	disabled

While authorizing user “John” in “sales” the fully qualified group name will be same as user DN like “CN=john,OU=sales,DC=nsna,DC=com”. But as Short Group Format is enabled and Short Group Attribute is configured as “OU”, group name will be extracted as “sales

User Interfaces Changes

[LDAP Menu]

servers	- LDAP servers menu
searchbase	- Set search base entry
groupattr	- Set LDAP group attribute
userattr	- Set LDAP user attribute
isdbinddn	- Set iSD bind DN
isdbindpas	- Set iSD bind password
ldapmacro	- User-defined macro menu
enaldaps	- Set Enable LDAPS
ldapscert	- Set LDAPS certificate
enauserpre	- Set Enable user preferences
enacutdoma	- Set Enable cut domain from user name
enashortgr	- Enable short group format
shortgroupattr	**- Set attribute used to extract short group**
groupsearc	- Group Search settings menu
timeout	- Set LDAP server timeout
activedire	- Active Directory settings menu
adv	- Advanced settings menu

New CLI item **shortgroupattr** in LDAP Menu allows to configure attribute to be extracted as group name from DN . Purpose of **Short Group Attribute** BBI configuration shown in **Figure 2** is same as shortgroupattr in CLI

Problems Resolved in This Release

CR Number	Description
Q02049592 Q02052599	**Title: NHA Applet Digital Signature Expired on Monday July 6, 2009** Description: The signed digital signature for the Nortel Health Agent (NHA) applet on NSNA is expired on Monday July 6th, 2009 at 08:00:00 PM local time to the client. After this time a client will be warned when executing the NHA applet that the signature has expired. Resolved this use by resigning NHA applet with a digital certificate having validity up to January 23rd 2011.
Q02049424	**Title: Delay in LDAP bind, search results in unexpected termination of EAP** Description: When Lightweight Directory Access Protocol (LDAP) search and bind request are delayed (due to the network/LDAP server performance) past the time out value of the Extensible Authentication Protocol (EAP) session, it results in managed crashes in EAP method implementations in NSNA server. It was causing authentication rejections. The root cause of the issue is identified as re-transmitted EAP packets by authenticator (switch) were not handled properly by NSNA server. Issue is resolved by handling the retransmitted EAP packets.
Q02041757	**Title: SNMP OID does not respond with correct number of Phone Sessions** Description: The SNMP query on oid .1.3.6.1.4.1.1872.2.3.2.3.1.1.4.2.4 was always returning 0 even if there were existing phone sessions. This issue has been introduced with a fix in NSNAS 2.1.1.0 release (CR Q02013586), which was done to avoid 100% CPU utilization in NSNAS server on SNMP query processing. Problem solved by correcting the mistakes in number of phone sessions calculation.

8. New Outstanding Issues

NA

9. New Known Limitations

NA

For other known issues, please refer to the product release notes and technical documentation available from the Nortel Technical Support web site at: http://www.nortel.com/support

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Technical Support on the web at: http://www.nortel.com/support

NSNA
Software Release 2.1.1.0

1. Release Summary

Release Date: May 2009
Purpose: Software maintenance release to address customer software issues.

2. Important Notes before Upgrading to This Release

NSNAS Software Upgrade Requirements:

NSNAS should have installed with version 1.6 or later before upgrade.

Saved Configuration file compatibility

In order to maximize configuration compatibility during upgrade, Nortel do not recommend upgrading from very old manufacturing releases like 1.0 or 1.5 to 2.1.1.0 based release. Please do interim upgrade to 2.0.X based release before upgrading to 2.1.1.0.

3. Platforms Supported

4050, 4070

4. Notes for Upgrade

File Names for This Release

File Name	Module or File Type	File Size (bytes) & MD5
NSNAS-2.1.1.0-upgrade_complete.pkg	Upgrade image	49,548,704 (bytes) 0ad6fa1cde09d8bd48f9ee308db67698
NSNAS-2.1.1.0-cdimage.iso.gz	Compressed ISO image	51,858,530 (bytes) 1ac65ae52c086ed064127cce9d2dca77
NSNAS_MIBs_2.1.1.0.zip	NSNAS SNMP MIBs	163,177 (bytes) 6914529a3ac08ea45667e4ee8eef1fb3
NSNAS_TPS-2.1.1.0.tgz	NSNAS TPS Module	7,612 (bytes) e8f20080aada7370bcdf0a8b8bc2674e
NSNAS-2.1.1.0-boot.img	NSNAS Network Boot image	49,521,226 (bytes) 376b4198e40f9d422747e3bd43d16888

5. Version of Previous Release

Software Version 2.0.1.2

6. Compatibility

Nortel Health Agent – 5.2.

7. Changes in This Release

New Features in This Release

NSNAS Stability Enhancements

These features are added to enhance the overall stability of NSNAS and to generate syslog/event/alarm messages to alert administrator for taking appropriate actions. The features include Overload protection, Health monitoring and Watchdog utility.

Avoiding and Managing Overload (Q01999210)
Nortel SNAS now has the feature for detecting, avoiding, and recovering from overload conditions. SNAS Server's overload protection features helps prevent the negative consequences—degraded application performance and stability— that can result from continuing to accept requests when the system capacity is reached.
The protection feature collects runtime statistics like current number of sessions, access switches that are handled per SNAS node within the cluster, System resources (CPU, Memory etc) utilization, and provide the decisions to authentication and switch management services within the SNAS. The decisions are based on algorithm that takes threshold configuration values and runtime statistics as input.

Self-Monitoring (Q01999211)
Nortel SNAS has added a feature to monitor self-health. A self-test task is executed at each configured interval. The task includes checking of software configuration, status of system resources (CPU, Memory, disk space etc) per node, memory used/opened files by Linux processes (Httpd, Simpleproxy, Erlang) . Self-monitor will generate appropriate syslog and alarms.

Watchdog (Q01999212)
Watchdog Timer is a piece of software that can cause a process or platform to reset when it judges that the system has hung, or is no longer executing the correct sequence of code. The watchdog is responsible for monitoring the critical processes within the Erlang virtual machine of a SNAS node. The suspicious processes are identified and appropriate alarm/syslog message is generated. The watchdog is capable of taking the first aid action on the hung process by killing it and making sure that the supervisors restart the process or the platform.

Restricting unsupported browsers (Q01998041)
This feature enables SNAS to allow portal login using only the supported browsers. Some of the browsers are currently not supported and a portal login using these results in an unexpected behavior. By enabling browser restriction feature, the user trying to do a portal login using unsupported browser will receive an error page instead of the normal portal login page.
The list of browsers supported can be updated in SNAS by importing a new browser signature file.
By default the browser signatures of supported browsers are preloaded in SNAS. However the feature is disabled by default.

Default Browser signature file
A default browser signature file is provided in SNAS. The file can be found under the directory /sac/priv/browser_signatures.txt. The contents of this file are loaded into registry when the system is upgraded or when a new image is loaded.
The browser signatures stored on SNAS can be exported to external system.

Browser signature file contents
The browser signature file is a text file. It contains entries of supported and unsupported browser signatures. Each line caters to a particular OS type of the browser. This is used as an index for internal operations.

The contents of browser signature file must be as below:

<Status>_#_<OS>_#_<Browser List>

Status will be supp – for supported browser version and Os type.
unsupp – for unsupported browser version and Os type.
OS – OS version of the browser.
Browser List - <Browser version1>,<Browser Version2>,…<Browser VersionN>

Adding new browser signature

To add new browser signatures the following steps must be followed:

Export the existing browser signatures using the cfg/domain <id>/portal/browsersig/export command. The file must preferably be exported as a text file with extension .txt.

Edit the file using any of the text editors. If the OS version of the browser is already present in the file, then the new browser version can be appended at the end of the line separated by a comma ",". If the browser OS version is not present a new line for that particular OS must be added.

Example: To add new entries for following browser list.

Supported browsers:

Browser name	Browser version	OS
Firefox	Firefox/2.0	Windows NT 5.1
Firefox	Firefox/3.0.0.8	Windows NT 5.1
Internet Explorer	MSIE 6.0	Windows NT 5.1

Unsupported browsers:

Browser name	Browser version	OS
Opera	Opera/9.62	Windows NT 5.1
Firefox	Firefox/2.0.0.11	Windows NT 5.1

To add these entries we need to add 2 new lines of this form:

```
supp_#_Windows NT 5.1_#_Firefox/2.0,MSIE 6.0,Firefox/3.0.0.8
unsupp_#_Windows NT 5.1_#_Opera/9.62,Firefox/2.0.0.11
```

The lines have the following meaning:
Browsers Opera/9.26 and Firefox/2.0.0.11 with OS version windows NT are not supported. Whereas Firefox version 2.0.x (with the exception of Firefox/2.0.0.11, as this is in the unsupported list), MSIE 6.0 and Firefox/3.0.0.8 with OS version Windows NT 5.1 are allowed.

NOTE: *The browser names must be comma separated and no blank space must be present between the names.*

```
supp_#_Windows NT 5.1_#_Firefox/2.0,MSIE 6.0, – correct
supp_#_Windows NT 5.1_#_Firefox/2.0,  MSIE 6.0,Firefox/2.0.0.18  - incorrect(blank space before MSIE 6.0)
```

Import the Edited file to SNAS.

Getting the browser Signatures (user agent ID)

Each browser identifies itself using a user agent ID. The browser name and version must strictly be as it is in the user agent ID.

For example for the user agent ID:
Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.2) Gecko/2008092313 Ubuntu/8.04 (hardy) Firefox/3.1

The browser name and version must be - Firefox/3.1
The OS will be - Linux x86_64

The user agent IDs can be found here: http://www.useragentstring.com/pages/useragentstring.php

Portal page customization (Q01975401)

A new configuration item has been added to the set of portal customization attributes. This command lets you specify a custom text to be displayed at the bottom of the Portal Login page, as an ordinary text string or as HTML code.

User-Interface changes

Stability Enhancements: A health menu is added to support the configuration of above mentioned stability features.

```
>> Main# /cfg/sys/adm/health
------------------------------------------------------------
[Health Menu]
      overload   - Avoiding and Managing Overload
      selfmon    - Self-Monitoring
      watchdog   - Watchdog
      default    - Set factory default settings for health monitoring

>> Main# /cfg/sys/adm/health/overload/
------------------------------------------------------------
[Overload Menu]
      cpulimit   - Set Cpu limit to reach overload
      memlimit   - Set Memory limit to reach overload
      maxsession - Set Maximum session limit to reach overload
      maxswitche - Set Maximum switch limit to reach overload
      blockswitc - Set Block switches on overload
      blocksessi - Set Block sessions on overload
      interval   - Set Statistics collection interval
      ena        - Enable Overload
      dis        - Disable Overload
      default    - Set factory default settings for overload protection

>> Main# /cfg/sys/adm/health/selfmon/
------------------------------------------------------------
[SelfMonitor Menu]
      cpulimit   - Set Cpu limit to monitor
      memlimit   - Set Memory limit to monitor
      dhcplimit  - Set Dhcp allocation limit to monitor
      disklimit  - Set Disk space limit to monitor
      switchlimi - Set Switches limit to monitor
      sesslimit  - Set Sessions limit to monitor
      interval   - Set Self monitor interval
      ena        - Enable SelfMonitor
      dis        - Disable SelfMonitor
      default    - Set factory default settings for self-monitoring

>> Main# /cfg/sys/adm/health/watchdog/
------------------------------------------------------------
[Watchdog Menu]
      interval   - Set Health check interval
      deadcnt    - Set Health check dead count
      action     - Set Autoremediate the system state
      ena        - Enable Watchdog
      dis        - Disable Watchdog
      default    - Set factory default settings for watchdog
```

Portal customization

```
>> Main# /cfg/domain 1/portal/
```

```
------------------------------------------------------------
[Portal Menu]
      import     - Import banner image gif
      restore    - Restores default Nortel banner
      banner     - Show installed banner file
      redirect   - Set redirect URL
      logintext  - Set static text on login page
      bottomtext - Set static text on bottom of the page
      iconmode   - Set Home tab icon mode
      linktext   - Set static text on link page
      linkurl    - Set url input field on link page
      linkcols   - Set number of columns on home tab
      linkwidth  - Set width of link columns on home tab
      companynam - Set company name used on portal pages
      colors     - Portal colors menu
      content    - Portal custom content menu
      lang       - Portal language menu
      ieclear    - Set use IE ClearAuthCache
      autoclose  - Set close authonly client portal automatically
      actimeout  - Set Auto Close Timeout for portal
      browsersig - Supported Browser Signature Menu
```

```
bottomtext <text string or HTLM code>
```

Lets you specify a custom text to be displayed at the bottom of the Portal Login page, as an ordinary text string or as HTML code.
Having entered the logintext command, type or paste the desired text. Press ENTER to create a new line and type "..." (without the quotation marks. Finally press ENTER once again.

```
>> Main# /cfg/domain 1/portal/browsersig
------------------------------------------------------------
[Supported Browser Signature Menu]
      ena        - Enable browser restriction
      dis        - Disable browser restriction
      list       - List all supported signatures
      import     - Import signatures from TFTP/FTP/SCP/SFTP server
      export     - Export signatures to TFTP/FTP/SCP/SFTP server
```

A new browsersig menu is added under /cfg/domain <id>/ portal menu. This menu allows you to manipulate the list of supported browser signatures by importing and exporting the list as an ASCII file.

Problems Resolved in This Release

CR Number	Description
Q01987288	**Title: New NSNA client access session still shows on previous port**
	Description: On creating new session, any existing sessions for the same MAC or IP are being deleted and old port will be reset. An improper handling in a function was made by wrong assumption that the new switch and old switch to be the same. That made port reset to be sent to old Port on new switch w. But expected was to sent to old switch old port. Problem solved by send the port reset to correct switch and port.
Q01987808	**Title: Disconnected ERS switches causes CPU spikes NSNA**
	Description: The SNAS tries to establish the connection with the switch by spawning a process. The process will exit if the switch is not available causing SNAS to restart the process. The starting of the process continuously causes the SNAS to utilize most of the CPU cycles. The new logic has been added to check for the reachability of the switch by pinging it and SNAS will attempt to establish only if the switch is reachable. Otherwise it will keep on checking for the reachability every 20 seconds.
Q01978915	**Title: NSNA Switch distribution failure due to "Out of ports" Error**
	Description: The Switch handling code on NSNAS has only 100 ports allocated for SSH connection to the edge switches. Customer has seen problems with 110 switches on site. Problem solved by increasing the limit on the NSNAS code to 2000 ports.
Q01978938	**Title: The NSNA command /info/dist does not work**

	Description: Root cause of the problem is same as Q01978915.
Q01941392	**Title: SNAS controller (1.6.1.3) does not show the remote link through SONMP**
	Description: Issue 1 – SONMP doesn’t start: when trunk is enabled with 2 or more ports under the interface tab NSNA creates the bond0 interface on the OS. The SONMP protocol code is not listening on the bond0 interface. Problem solved by adding the code to correctly detect and attach to the interfaces.
	Issue 2 – Zero Linkup to 8300: The hardcode value in the protocol implementation is causing the problem. SONMP protocol code on NSNAS has been modified to use the response value to solve this problem.
Q01965850	**Title: Switch Incompatible message in starttrace log**
	Description: Incorrect log message. The trace message is modified to display the correct message. 1). When a user login from SSCP-Lite switch and TG mode is never, which is not supported. 2). User login from either SSCP or SSCP-Lite switch from unmanaged port. New Message : "Either SSCP-Lite switch incompatible with NHA mode - never or logged in from unmanaged port; Logout user [user name] "
Q01950254	**Title: SNAS-2.0.1: Captive portal not working after disable/enable HTTP Redirect via BBI**
	Description: BBI is not setting a registry value while enabling Http Redirect from BBI.
Q01966580	**Title: Excessive SSL Request created by the Web Browser with Auto Proxy configured**
	Description: Upon configuring automatic web proxy in the Web Browser User Agent causes the GET /wpad.dat HTTP/1.1\r\n requests for the proxy auto config file. As expected a HTTP 301 redirection is sent by the SNAS, hence the Browser attempt to connect via HTTPS. The browser never gets to send the GET request in the HTTPS connection as the HTTPS session is limited to just the SSL handshake. Hence the process iterates continually until the page is fully loaded via two separate HTTP sessions. This gives a slow portal page performance perspective to the customer. SNAS will send an HTTP_STATUS_OK message for the wpad request along with the required data. This will be done from simpleproxy itself.
Q01974813 Q01974813-01	**Title: NSNA :Sometimes PC connected behind phone gets red filter**
	Description: Sometimes when the MAC trusted PC is shutdown/disconnected and started again after a few hours, the PC gets the red filter and won't be able to access the resource. At the same time the PC has a green session on SNAS. The fix is to re-create the cache entry when received the MAC authentication request for the existing session.
Q01974702	**Title: Dead lock loop when authenticating to the NSNA Server**
	Description: Analyses of system backtrace and logs from outage revealed possible deadlock scenario between SAC & AAA servers on NSNA. Those servers (processes) are responsible for switch control & user authentication. Since connectivity between nodes in cluster was not lost, failover did not happen. Also servers did not restart since they were not actually dead or crashed and appeared normally functioning from system point of view. Code analyses revealed possible additional scenarios of such deadlocks in those servers. Blocking system calls that were responsible for deadlock were replaced with non blocking calls with appropriate handling in all suspected places.
Q01993190	**Title: Sometimes SNMP query to the SNAS returns EXIT**
	Description: The root cause of the problem is related to Q01994393.
Q01992696	DHCP setting for filter only user doesn't change when move from ipphone to other
	Description: SNAS manages information about the devices connected on the switch ports. When a device is moved between the switches the old switch-port association was used instead of the new switch-port. Problem is fixed to use the correct switch-port information when the device is moved. The fix is related to Q01994070.
Q01993756	**Title: Erlang server crash forcing MIP ownership change**
	Description: The root cause is related to Q01994393.

Q01982758	**Title: Logging out process fails with Mac OSX clients**
	Description: When user clicks logout link, portal issues logout request to SNAS, and on unload of the current page portal instructs NHA to do DHCP release/renew. On MAC OSX Browsers "on unload" event of portal is not working as expected. Also in some cases "on unload" is triggered well before user logout process at SNAS side is complete (i.e before flip VLAN) and DHCP release/renew resulted in green IP itself. The assumptions made on sequence of events/timings and browser behavior resulted in this issue. The fix is to trigger logout as well as DHCP release/renew through a single API in NHA (already existing) and portal does not issue logout directly to SNAS. Hence DHCP activities happen properly after user logout. This fix is applicable for portal authentication with NHA only, if NHA is not used (auth only mode) logout is issued by portal, but as there is no DHCP activities it works fine as before. The login was failing in safari because, in case of MAC login successful page was requested before VLAN/filer change and DHCP release renew, and it is purely because of behavior of MAC browsers.
Q01993175	**Title: BBI/Erlang: High SNAS controller memory use on the MIP owner.**
	Description: The issue lies in the interfaces (between the PHP and Erlang Shell) that BBI uses to communicate with the back end. The major leak was pin pointed in libisderlang.so.0.1 which is built as a result of erl_wrapper.cpp. The memory was not released properly in this file. The zend wrapper called from PHP in turn calls the objects defined in erl_wrapper.cpp for rpc_calls. The updates have been incorporated in SNAS code, and noticed a drastic reduction in the memory consumption in our device.
Q01998731	**Title: SNAS Mac OS Users Continually Logged Out**
	Description: NHA minimum version check is causing the NHA seesion to terminate in the events of waitheart beat and recheck interval. Version check is now restricted to only at the new session creation and at restart_session.
Q01982540	**Title: SNAS cluster reported SNMP cold start traps.**
	Description: Fixes the handling of the malformed packets. If the userID= /\..\..\..\..\..\boot.ini(anything) & UserId= abc@cde@fgh@xyz causing the radius server crash. On fresh installed nodes, this authentication attempt is causing the crash & one snas node is getting reinitiated. Modified the DNS server to handle the queries on TCP port.
Q02004309	**Title: Phones disappear from SNAS CLI/BBI after switch reboot**
	Description: The issue is related to failopen functionality in the ERS code. The new changes in the ERS for failopen fixes the issue.
Q02013586	**Title: SNAS : SNMP queries results in high CPU (100%) on MIP owner**
	Description: The implementation for fetching session type count calculation was not efficient during SNMP get. Optimized the code to calculate session type count. Also have removed unnecessary logs. CPU usage is now normal with the optimized code.
Q01992699	**Title: NSNA filter user get stuck with known filters when moving from ipphone to switch**
	Description: Using portal login, if a PC is moved from one port to another, old session is not getting deleted. The same behavior is observed in case if the PC is connected behind the phone. The new port could be on the same switch or on a different switch. The problem was that during the lookup of a MAC, the old switch/port association was used instead of the new one.
Q01993180 Q01993183	**Title: Logging in process fails with Mac OSX clients**
	Description: MAC OSX 10.5 running safari 3.2.1 is behaving differently than Windows browser based NHA functionality. Here the portal login-success page is requested before the VLAN/filter change on the switch and the machine getting the new IP address, causing the browser to display the timeout page. Problem solved by introducing a delay (2 sec) in fetching the login success page to allow the switch to change VLAN/filter and PC to do DHCP.

Q01994393	**Title: SNAS : DNS service is getting restarted continuously**
	Description: A condition where multiple entries in the AAA cache are seen for the same client IP address which is causing the DNS service to restart. DNS Service is fixed to handle of multiple AAA cache entries. The disconnection between the nodes causes the RPC calls from node to other node fail, causing one node to think that client session is not existing. There is an additional check added to detect the multiple AAA cache entries and delete if there is an old one.
Q01987279	**Title: Mac authenticated user can't connect behind an IP phone after 1st user timed out**
	Description: On receiving the MAC authentication request for a MAC from a switch, if there is already an existing session for that MAC on a different switch, the session related to original switch is not getting deleted. This behavior is observed if the Pc device is connected behind a VOIP phone. The result is that there are duplicate session entries for the same MAC but on different switch/port. Problem solved by adding code to look for session even if the PC is connected behind the phone.
Q02027169 Q02028010	**Title: NHA client icon is green after the Session is terminated**
	Description: In an NSNA 802.1x solution, the Installed NHA client icon stays green after the NSNA session has been terminated or the Tun/Tap adapter has been disconnected form the PC. The issue has been resolved by updating the icon color to grey if network connection is down.

8. New Outstanding Issues

Case 090415-20429 “Occasional close of control sessions between SNAS & 5520s”

9. New Known Limitations

CR Number	Description
Q02008081 Q02008592	Admin Applet:Double trigger action appears in Trigger action in SRS rule
Q01993362	Title: PC Behind Phone: Phone does not get VOIP IP if PC is connected behind it
	Description: The switch could learn the PC MAC before the Phone establishes the connection with the call server and move the port from RED VLAN to authenticated VLAN. The phone related DHCP parameters should be replicated from RED subnet to GREEN and YELLOW subnets to address this.
Q01996938	Title: SNAS 4050: RADIUS Process stopped on SNAS controller.
	Description: One time occurrence with unknown trigger. In 2.1 Radius Process will restart if stopped. (Enhancement request Q01999212)
Q02000411	Title: SNAS AAA crash with high scaling sessions.
	Description: One time occurrence with unknown trigger. In 2.1 AAA Process will restart if stopped. (Enhancement request Q01999212)
Q01998440 Q01994633	Title: Portal never times out if move filter_only DHCP PC from behind phone Title: IP does not update in /info/switch when PC behind phone is swapped
	Description: This is the limitation from DHCP client on the PC. If the PC is moved in less than 15 sec the DHCP client of PC may not renew the IP address. IP release/renew on PC or admin down/up of switch port can be used to correct this.
Q01997669	Title: NSNA 2.0 - Portal Login fails with Safari 3.2.1 browser in Windows XP.

	Description: Currently only IE and Firefox browsers are supported on Windows. Please refer to the support matrix for OS and browsers versions in 2.0.1.2 release notes
Q01993365 Q01996411	Title: Mac Authenticated session not tearing down when client is shut down Title: PC behind phone: Mac auth session not deleted if PC unplugged/disabled
	Description: SNAS allow only two devices on any NSNA enabled port - 1 VOIP phone and 1 static or DHCP IP based device. For MAC authenticated clients, as soon as the MAC is learned on the switch, the session gets created on the SNAS (and a license will be consumed). This session remain active till 1) session times out 2) a new MAC is learned on the same port 3) this MAC is learned on a new port There is an age out interval associated with each MAC that switch learns on the port. By default the age out interval is 5min. So, if a MAC1 is authenticated (and session is created on the SNAS) on port1, the switch won't allow the second MAC (MAC2) to go through. The traffic from the MAC2 will remain blocked as long as the MAC1 remains learned and is not idle. If MAC1 is unplugged, the MAC2 will be able to gain access if it is authenticated and the session for MAC1 will be deleted.
Q01994657	Title: SRS re-check happens before the re-check interval
	Description: The agent keeps on checking for the change in status. At any point if it detect that the PC scan status has changed, it will force server to perform the entire scan cycle. It should not wait for expiration of the re-check interval. The re-check interval is the interval at which server asks agent to perform the scan.
Q01996406	Title: PC behind phone: Mac auth session remains even if Mac deleted from MAC db
	Description: On the fly removal of MAC entries from MAC database are not supported. Manual kick of sessions is required from SNAS
Q01997187	Title: Failure info is not showed in the Policy tab dynamically
	Description: For NHA, valid messages are dynamically updated in "status" tab, but no failure message is displayed in "policy" tab, the status window has to be closed and re-opened again for policy tab to be updated.

For other known issues, please refer to the product release notes and technical documentation available from the Nortel Technical Support web site at: http://www.nortel.com/support

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Technical Support on the web at: http://www.nortel.com/support